

SECRETARÍA : Criminal

PROCEDIMIENTO : Especial

RECURRENTE (1) : Moisés Sánchez

RUT N° : 11.867.591-6

RECURRENTE (2) : FUNDACIÓN KAMANAU

RUT N° : 65.206.289-k

ABOGADOS

PATROCINANTES Y APODERADOS (1) : Ciro Colombara López

RUT N° : 10.220.552-9

(2) : Aldo Díaz Canales

RUT N° : 15.335.526-6

DOMICILIO : Alonso de Córdova N° 4355, piso 14,
Vitacura

RECURRIDO : Worldcoin

REPRESENTANTE (1) : Sam Altman

REPRESENTANTE (2) : Felipe Esteban Ayala Sanhueza

RUT : 18.078.329-6

DOMICILIO : Avenida Providencia Nro. 1650, OFICINA
611, comuna de Providencia, Región
Metropolitana.

CORREO : fayala@worldcoin.org

EN LO PRINCIPAL: Interponen Acción de Protección; **PRIMER OTROSÍ:** Solicitan se decrete orden de no innovar; **SEGUNDO OTROSÍ:** Acompañan documentos, con citación; **TERCER OTROSÍ:** Patrocinio y poder; **CUARTO OTROSÍ:** Señalan direcciones electrónicas.

ILTMA. CORTE DE APELACIONES DE VALPARAÍSO

CIRO COLOMBARA LÓPEZ y ALDO DÍAZ CANALES abogados, en representación, de **MOISÉS SANCHEZ RIQUELME**, cédula de identidad N° 11.867.591-6 **por sí**, y en representación de FUNDACIÓN KAMANAU, RUT 65.206.289-k, con domicilio legal en la comuna de Isla de Pascua, Región de Valparaíso; todos los comparecientes domiciliados para estos efectos en calle Alonso de Córdova N° 4355, piso 14, comuna de Vitacura, Santiago, a S.S. Iltma., con respeto decimos:

Que, estando dentro de plazo y de conformidad a lo dispuesto en el artículo 20 de la Constitución Política de la República (en adelante, "**CPR**"), en relación con lo dispuesto en el Auto Acordado sobre Tramitación y Fallo del Recurso de Protección de las Garantías Constitucionales dictado por la Excm. Corte Suprema (en adelante, "**Auto Acordado**"), venimos en deducir recurso de protección en contra de la empresa **WORLDCOIN SpA** (en adelante; "**WORLDCOIN**"), **RUT 77.318.452-6**, con domicilio en Calle La Capitanía 80, Oficina 108, piso 1, Comuna de Las Condes, Región Metropolitana, representada legalmente en el territorio nacional por **FELIPE ESTEBAN AYALA SANHUEZA**, cédula nacional de identidad **Nro. 18.078.329-6**, con domicilio en Avenida Providencia Nro. 1650, oficina 611, comuna de Providencia, Región Metropolitana; **en virtud de la recolección por parte de dicha empresa de datos biométricos de nuestro representado a través de una fotografía del iris ocular a cambio de criptomonedas, ocurrido con fecha 13 de marzo de 2024, en la ciudad de Viña del Mar.**

En términos simples S.S. Iltma., el escaneo de iris por parte de WORLDCOIN a cambio de criptomonedas es un acto ilegal ya que infringe: **(i)** El artículo 4 inciso primero y segundo de la Ley N° 19.628; **(ii)** El artículo 11 de la Ley N° 19.628; y, **(iii)** El artículo 13 de la Ley N° 19.628.

Además de ser ilegal, el acto recurrido es arbitrario ya que obedece al mero capricho de la empresa recurrida. Asimismo, el acto recurrido carece de razonabilidad.

El acto recurrido, además de ser ilegal y arbitrario, vulnera el legítimo ejercicio de las siguientes garantías fundamentales de las que es titular

nuestro representado y que se encuentran amparadas en el artículo 20 de la CPR: **(i)** Garantía de que el desarrollo científico y tecnológico estén al servicio de las personas y con respeto a la vida y a la integridad física y psíquica; **(ii)** El derecho a la vida privada, garantizado en el artículo 19 N° 4 de la CPR; y, **(iii)** El derecho a la propiedad, garantizado en el artículo 19 N° 24.

Así, solicitamos a S.S. Iltma., tener por interpuesta la presente acción de protección en contra de WORDLCOIN, declararla admisible, solicitar informe al representante legal de la recurrida en Chile a través del correo electrónico fayala@wordlcoin.org dentro del plazo de 5 días y, en definitiva, acogerla en todas sus partes, ordenando lo siguiente: **(i)** Que, la empresa recurrida modifique sus políticas de privacidad en lo concerniente a la protección de los datos biométricos; **(ii)** Que, la empresa recurrida se abstenga de obtener datos biométricos mediante fotografías del iris mientras no modifique sus políticas de privacidad; **(iii)** Que, la empresa recurrida elimine de su base de datos la información biométrica de nuestro representado; **(v)** Que, se adopten todas las demás medidas que se estimen necesarias para restablecer el imperio del derecho; y, **(vi)** Que, se condene expresamente en costas a la empresa recurrida.

En definitiva, fundamentos el presente recurso de protección en los argumentos de hecho y de derecho que, a continuación, pasamos a exponer:

I. ANTECEDENTES DEL SR. MOISÉS SÁNCHEZ:

1. El recurrente es Director Ejecutivo de FUNDACIÓN KAMANAU, una organización de la sociedad civil que tiene por objetivo velar por la protección de los derechos humanos en el contexto de las nuevas tecnologías. Por esta razón presta atención a todos los nuevos desarrollos tecnológicos que van surgiendo.
2. Nuestro representado se define como un explorador, amante de lo diferente y las fronteras. Desde el mundo del derecho y el periodismo busca revelar lo que esta oculto, y velar por el respeto de los derechos humanos. Amante de la música y el baile, los libros de aventuras y de ciencia ficción. Durante años trabajó en Libertad de Expresión y Acceso

a la Información, y hoy tiene puesta la mirada en los desafíos de futuro que representan los avances científicos y las tecnologías disruptivas.

3. FUNDACIÓN KAMANAU es una organización de la sociedad civil que busca proteger los derechos humanos frente al avances de las tecnologías disruptivas. Dentro de sus áreas de trabajo se encuentran la inteligencia artificial, los neuroderechos, las experiencias inmersivas metaverso, y la edición genética. <https://kamanau.org/>

II. ANTECEDENTES DE WORLDCOIN:

4. WORLDCOIN es una empresa domiciliada en las Islas Caimán que ha desarrollado una operación internacional consistente en recolectar datos biométricos de las personas a través de una fotografía del iris ocular.
5. El objetivo de la empresa recurrida es reunir datos biométricos para crear una red financiera y de identidad global. En este sentido, la empresa ha explicado que el proyecto pretende emitir un documento de identidad digital que demuestre de una manera infalible que el titular es una persona y no un "bot" o robot informático.¹
6. Según se ahondará en esta presentación, WORLDCOIN ha instalado puestos a lo largo de todo el mundo -incluido Chile- en donde los usuarios pueden escanear su iris a cambio de la entrega de criptomonedas, una moneda digital.
7. Con respecto a la conformación de la empresa recurrida, la página web de WORLDCOIN señala que la entidad estaría respaldada por una comunidad global de desarrolladores, economistas y expertos en tecnología, y que la WORLDCOIN FOUNDATION es el administrador inicial del protocolo.²

¹ <https://www.biobiochile.cl/noticias/economia/negocios-y-empresas/2024/03/11/alerta-en-europa-por-firma-que-pide-escanear-iris-a-cambio-de-bono-en-chile-capto-a-miles-de-personas.shtml>

² Página web de Worldcoin, sección preguntas frecuentes. Disponible en: <https://es-es.worldcoin.org/faqs>

8. Consultada la página web de la WORLDCOIN FOUNDATION, en su sección de "Learn more", se lee que la fundación está incorporada en las Islas Caimán, y que no tiene miembros, es decir, que no tiene dueños ni accionistas.
9. La página web señala que la fundación está gobernada por una junta de tres directores: Chris "W" Waclawek, Phillip Sippl, y "otro director profesional domiciliado en Islas Caimán".³ Obsérvese la siguiente captura de pantalla de la página web:

The Worldcoin Foundation is an exempted limited guarantee foundation company, which is a type of non-profit, incorporated in the Cayman Islands. To learn more about this type of entity, check out this [Guide to the Cayman Islands Foundation Company](#) from the Foundation's outside counsel at the law firm Ogier.

The aim of the Foundation is both philosophical and political: to realize more inclusive, fair, and just institutions of governance and of the global digital economy, including by helping achieve certain targets of U.N. Sustainable Development Goal 16 (namely, 16.4, 16.5, 16.6, 16.7, and 16.9). To that end, it serves as the steward of the Worldcoin protocol, supporting and growing the ecosystem until it becomes self-sufficient.

Today, the Worldcoin Foundation is "memberless"; it has no owners or shareholders. It is governed by a Board with three Directors, Chris "W" Waclawek, Phillip Sippl, and another Cayman Islands based professional director.

10. De acuerdo a los *Articles of Association de Worldcoin Foundation*, la sociedad tenía miembros iniciales, que eran los suscriptores de tal documento (artículo 3.1), pero podía pasar a convertirse en una sociedad sin socios (artículo 3.5):

3 Members

First Members

3.1 The subscribers to the Memorandum are the first Members of the Company.

EXEMPTED Foundation
filed as No. 395
Assista

³ Worldcoin Foundation (2023). Sección "Lean More", bajo el título de "Worldcoin Foundation". Disponible en: <https://www.worldcoin.foundation/information>

Company may be without Members

3.5 It is not a condition of this Article 3 that the Company continues to have one or more Members.

11. Pues bien, la única suscriptora de los Articles of Association fue la compañía Leeward Management Limited, radicada en Islas Caimán (primera socia). Sin embargo, según se indicó, la página web de WORLDCOIN anuncia que la sociedad ya no cuenta con ningún/a socio/a.
12. Debe destacarse que, además, la compañía tampoco tiene un domicilio fijo, pues, de acuerdo al artículo 8 de su Memorandum of Association, su localización corresponderá a la dirección de negocios del secretario, durante su ejercicio.

III. DEL WORLD ID:

13. Worldcoin ha desarrollado un sistema de identificación llamado World ID. Utiliza una tecnología especial denominada biometría del iris para asegurarse de que cada persona sea única en el mundo digital. Esto significa que al usar World ID, las personas pueden demostrar que son humanos reales y únicos, y no robots o programas automáticos. "Con su World ID, podrá iniciar sesión para autenticarse en aplicaciones web, móviles y descentralizadas, y compartir de forma privada sus verificaciones personales, incluida la biometría, para obtener el máximo nivel de seguridad", señala la empresa en su sitio web⁴.
14. Para comenzar, las personas deben descargar una aplicación llamada World App. Esta aplicación les permite crear su World ID. Luego, visitan un dispositivo físico llamado Orb, que se encuentra en lugares de acceso masivo como centros comerciales y estaciones de metro en el caso de Chile. Este Orb escanea los iris de las personas para verificar su identidad única. "El único camino para verificar la unicidad a escala global es la biometría del iris"⁵ señala la empresa en su whitepaper.

⁴ <https://support.worldcoin.com/hc/es/articles/15443486098323--Qu%C3%A9-es-World-ID>

⁵ <https://whitepaper.worldcoin.org/proof-of-personhood>

15. Una vez confirmada la identidad, el Orb emite un código numérico que sirve como la identificación mundial verificada por Worldcoin. Este código solo se emite una vez para cada persona, garantizando así su unicidad.
16. Una vez obtenida la identificación única, ésta se registra en la blockchain (cadena de bloques), y las transacciones u operaciones que se hagan con esta identidad digital quedarán registradas ahí por siempre. ***“Si esta verificación tiene éxito, la clave pública de World ID se inserta en un conjunto de identidades mantenido por un contrato inteligente en la cadena de bloques Ethereum. Posteriormente, el estado actualizado se conecta a Optimism y Polygon PoS para que World ID se pueda usar de forma nativa en esas cadenas”***⁶
17. Entonces, ¿por qué es relevante esta conexión con la blockchain? Primero hay que tener presente que la blockchain es como una cadena de eslabones de cuentas digitales que está distribuido en muchas computadoras en todo el mundo. Cada eslabón de esta cadena (llamada bloque) contiene una lista de transacciones. Cuando se agrega un nuevo eslabón se conecta al anterior formando una cadena, de ahí el nombre "blockchain".
18. **Lo importante es que una vez que un eslabón se agrega a la cadena (blockchain), no se puede cambiar sin que todos los demás en la red lo noten pues es de acceso público.** Así que, cuando World ID emite un código para una persona y la registra en la blockchain, toda la información de las transacciones efectuadas **quedará registrada por siempre de manera pública, sin posibilidad de ser eliminadas.** Esto es algo que la empresa no informa de manera adecuada por las razones que explicaremos más adelante.

IV. DE LAS POLITICAS DE PRIVACIDAD DE WORLDCOIN:

⁶ <https://whitepaper.worldcoin.org/technical-implementation>

a) Vulneraciones a la privacidad por parte de WorldCoin:

19. La empresa Worldcoin promete en su página de inicio ser una red financiera y de identidad humana que protege la privacidad a gran escala⁷. Sin embargo, esta promesa de privacidad carece de detalles específicos, lo que lleva a que las personas tomen decisiones sin tener toda la información necesaria, dada la ausencia de un consentimiento informado.
20. **Es importante destacar que esta garantía de privacidad de la empresa sólo alcanza a los datos biométricos crudos del iris obtenidos a través de los dispositivos de Worldcoin.** Sin embargo, la empresa no explica a sus usuarios claramente que sus derechos de rectificación o supresión no pueden ser ejercidos una vez que el código generado se registra en la blockchain, ni respecto de todas las operaciones relacionadas con la identificación efectuadas a partir de ese momento. Sin una explicación detallada de estos aspectos, los usuarios ven afectadas su capacidad para tomar decisiones informadas sobre su participación en la plataforma de Worldcoin.
21. La blockchain, al ser pública e inmodificable, no permite alterar o eliminar la información registrada en ella. La empresa misma reconoce esta limitación en el art 11 de su Biometric Data Consent Form: "las cadenas de bloques son redes descentralizadas de terceros que no controlamos ni operamos. Debido a la naturaleza pública e inmutable de la tecnología de cadena de bloques, no podemos modificar, borrar o controlar la comunicación de los datos que se almacenan en cadenas de bloques."⁸
22. Esto es especialmente relevante si consideramos que este método de identificación se puede utilizar en una serie de aplicaciones de uso masivo, tales como Mercado libre y Shopify (comercio electrónico),

⁷ <https://es-es.worldcoin.org/>

⁸ <https://vault.pactsafe.io/s/8a18d792-fd76-44db-9b92-b0bb7981c248/legal.html#contract-syn0uxpen>

Minecraft (juego en línea), Telegram (plataforma de mensajería), todas las cuales están habilitadas en Chile para operar con este sistema⁹.

23. Desde esta perspectiva, el consentimiento de los usuarios juega un papel crucial. Sin embargo, la forma en que la empresa obtiene este consentimiento no garantiza la adecuada información de los usuarios. Además, el uso de incentivos monetarios para fomentar la incorporación al sistema, como los Worldcoin Grants, plantea preocupaciones adicionales. Estos incentivos, que pueden ascender a una suma significativa de dinero, pueden influir en la decisión de los usuarios sin que estén completamente informados sobre los riesgos y consecuencias de participar en el sistema.
24. WorldCoin señala que *"a través de World ID, pueden reclamar una cantidad determinada de WLD periódicamente (Worldcoin Grants), cuando las leyes lo permitan"*¹⁰. **A la fecha de esta presentación, estos incentivos ascienden a la suma aproximada de \$90.000 pesos chilenos que se entregan en criptomonedas de propiedad de la empresa, los que se van incrementado en el tiempo según una serie de reglas de incentivos que establece la compañía.** Estos se pueden retirar a través de un procedimiento simple.
25. **Es importante considerar que la protección de la privacidad y el consentimiento informado son principios fundamentales en el ámbito de la tecnología y los datos personales.** En este caso, hay falta de transparencia y una coerción en la obtención del consentimiento de los usuarios, lo que compromete sus derechos y libertades fundamentales.
26. Adicionalmente, los fines que pretende la empresa no son claros. Como señaló en una reciente entrevista Mar España, directora de la agencia de protección de datos de España *"esos datos pueden ser utilizados en el futuro para suplantar la identidad de una persona, para tomar decisiones relacionadas con la salud (optar o no a un seguro médico)*

⁹ <https://techcrunch.com/2023/12/13/worldcoin-integration-reddit-telegram-shopify/?guccounter=1>

¹⁰ <https://whitepaper.worldcoin.org/technical-implementation>

y para que sean conscientes de que, aunque pueda parecer gratuito e inocuo, la cesión de este tipo de datos 'puede condicionar su futuro'.¹¹ Señala WolrdCoin en su Privacy Notice (punto 8) "Los datos, incluida su información personal, pueden ser compartidos entre nuestras empresas matrices, filiales y subsidiarias actuales y futuras y otras empresas bajo control y propiedad común". **Esto deja la puerta abierta para que la información sea utilizada para fines no declarados.**

27. **Por último, hay que hacer una mención especial al rol del Estado frente a la irrupción de nuevas tecnologías que pueden poner en riesgo los derechos de las personas.** Existen muchos países que han prohibido la recopilación de datos biométricos por parte de WorldCoin de sus ciudadanos (como es el caso de España), y en Estados Unidos la compañía no puede operar justamente por el vínculo que tiene su sistema de identificación digital con los criptoactivos, pues estima que se pueden utilizar como vehículo para la especulación y el fraude¹², entre otros posibles riesgos.
28. En efecto, tal como señaló la Excelentísima Corte Suprema en la sentencia del caso Girardi vs Emotiv (Rol 105.065-2023):
- "...ante la llegada de una nueva tecnología como la que es objeto de autos, que trata de una dimensión que antaño era absolutamente privada y personal, tratada en entornos estrictamente médicos, como es la actividad eléctrica cerebral, se hace absolutamente menester que previo a permitirse su comercialización y uso en el país, sean esta tecnología y dispositivos analizados por la autoridad pertinente, entendiendo que plantea problemáticas no antes estudiadas por ella".*
29. Las mismas consideraciones expresadas por la Excm. Corte respecto de los dispositivos neurotecnológicos, son aplicables al presente caso.

¹¹ La Agencia de Protección de Datos prohíbe a Worldcoin seguir recopilando en España datos del iris. 6 de marzo 2024. Disponible en <https://efe.com/economia/2024-03-06/aepd-prohibe-worldcoin-seguir-recopilando-espana-datos-iris/>

¹² <https://www.ft.com/content/b7a867f4-2462-4d1b-a805-b821bf0804f6>

30. En un sistema tan complejo y poco transparente, que expone a tantos riesgos y no es claro respecto de sus finalidades, no es razonable traspasar la responsabilidad de evaluar de manera informada a las personas. En su lugar, debe ser la empresa la que provea todos los mecanismos necesarios para lograr un consentimiento informado de alto estándar por parte de los usuarios, y el estado debe generar políticas que busquen proteger los derechos de las personas.

b) Ausencia Consentimiento informado:

31. El principio fundamental que rige el tratamiento de datos es el de licitud, que actúa como base legal necesaria para la recolección y tratamiento de los mismos. Esto implica que sin una causa que habilite el tratamiento, los datos no pueden ser tratados. En el caso presente, el consentimiento otorgado por los usuarios emerge como la puerta de entrada a la herramienta, siendo esencial para la legitimidad del procesamiento de datos.

32. En primer lugar, el responsable del tratamiento de datos debe priorizar la protección de los intereses del titular y abstenerse de obtener datos de manera fraudulenta. La recolección de datos de forma sorpresiva o engañosa no cumple con los estándares de protección de datos y se considera desleal según los estándares Iberoamericanos de Protección de Datos, especialmente si conduce a una discriminación injusta o arbitraria contra los titulares.¹³ La estrategia de la empresa, orientada a captar usuarios de mediante incentivos económicos, en lugares de alto tránsito de personas, y un sistema de obtención del consentimiento en su aplicación telefónica es del todo insuficiente, constituyendo una grave falta a este principio.

33. En segundo lugar, es fundamental garantizar la transparencia y claridad en la información brindada antes de la recolección de datos, asegurando que el titular conozca la **finalidad** del tratamiento. En este sentido, la empresa no entrega información previa a sus usuarios

¹³ art. 15 estándares Iberoamericanos: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

respecto del registro de su identificación en la blockchain, ni explícita de manera clara que su modelo de negocio no es sólo de identificación digital, si no que también de generación y gestión de criptoactivos.

34. En tercer lugar, el consentimiento informado es especialmente crucial en el ámbito de la salud, ya que está intrínsecamente ligado a la noción de personalidad y legitimidad para intervenir en datos sensibles. Por lo tanto, toda persona expuesta, incluso voluntariamente pero motivada por una contraprestación, debe tener la capacidad de autorizar consciente, deliberada e informadamente la entrega de sus datos sensibles, especialmente los datos biométricos.
35. Antes o en el momento de la recopilación de datos, se deben especificar claramente la identidad y datos de contacto del responsable, las finalidades específicas del tratamiento, el fundamento jurídico que legitima el tratamiento, los destinatarios o categorías de destinatarios de los datos, así como los derechos del titular en relación con los datos a recopilar. Cuando el tratamiento se base en el consentimiento, éste debe ser previo, inequívoco, libre e informado, mediante obtenido un proceso que garantiza la comprensión, con un enfoque intercultural y de género.
36. En conclusión, la empresa WorlCoin no ha cumplido con los requisitos del consentimiento informado, como se evidencia por las siguientes razones: a) no cuenta con mecanismos adecuados para obtener un consentimiento previo, inequívoco, libre e informado de los usuarios, considerando la naturaleza biométrica de la información recopilada y los riesgos: b) no ha garantizado la transparencia y claridad en la información proporcionada antes de la recolección de datos, especialmente en relación al impactos del registro del código de identificación en la blockchain, c) no ha explicitado de manera sencilla al usuario que no puede ejercer su derecho de rectificación o revocación del consentimiento respecto de la información que se registra en blockchain, y d) ha recopilado datos de manera desleal y coercitiva, sin respetar los estándares de protección de datos ni las normativas internacionales.

c) Vulneraciones principio finalidad. Imposibilidad de ejercer derecho a la supresión:

37. La finalidad es uno de los principios fundamentales del derecho a la protección de datos personales. En este sentido, la solicitud de datos debe tener fines justos, que persigan aquella finalidad para la que se recolectaron. Es un límite básico del estado de derecho.
38. El artículo 17 de los estándares iberoamericanos establece que todo tratamiento de datos personales se limitará al cumplimiento de finalidades determinadas, explícitas y legítimas. En nuestro caso, las finalidades no son explícitas, lo que hace cuestionable la recolección de dichos datos.
39. No encontramos precisiones de la empresa acerca de la finalidad en la recolección de datos biométricos sensibles, donde los extremos en materia de seguridad y control deben ser extremos, como así también la justificación de su recolección para determinados fines legítimos.
40. Por otra parte, la implementación del sistema de identificación digital y generación de criptoactivos de WorldCoin imposibilita ejercer el derecho de rectificación o supresión de datos por parte de los usuarios. En efecto, la expectativa de privacidad que ofrece la compañía no se corresponde a la realidad, ya que la infraestructura propuesta registra el código de identificación en la blockchain -por su naturaleza inmodificable-, así como todas la información sobre actividades y/o transacciones realizadas con éste, sin la adecuada información al usuario.
41. En este sentido, entendiendo que el derecho a la privacidad es un derecho humano, se destaca puntualmente en el informe sobre "*El derecho a la privacidad en la era digital*"¹⁴ que es innegable que las tecnologías basadas en datos pueden destinarse a usos altamente beneficiosos, pero estos avances tecnológicos plantean riesgos muy importantes para la dignidad humana, la autonomía y la vida privada,

¹⁴ Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (2018).

así como para el ejercicio de los derechos humanos en general, si no se gestionan con sumo cuidado.

42. En conclusión, la falta de claridad de la empresa respecto de los fines y la ausencia un consentimiento informado en el contexto de la implementación de sistemas de identificación digital, especialmente en relación a la información sobre la supresión de información y el control sobre los datos, vulnera los derechos fundamentales de las personas y pone en riesgo su dignidad, autonomía y libertad.

d) Falta de debida diligencia de la empresa:

43. En el caso que nos ocupa, la empresa WorldCoin no da cuenta del cumplimiento de las reglas previas que establezcan un marco de confianza para los desarrollos relacionados con la identidad digital a través de datos biométricos. Esto resulta preocupante, ya que la falta de transparencia en la definición y cumplimiento de estas reglas puede representar una amenaza para la protección de los derechos de los usuarios y la integridad de los sistemas de identidad digital.
44. En efecto, los marcos de confianza son conjuntos de reglas, estándares y procedimientos que establecen un marco de referencia para garantizar la seguridad, privacidad y confiabilidad de los sistemas de identidad digital. Buscan asegurar que el diseño y la implementación de estos sistemas estén centrados en el usuario. Esto implica evaluar la conveniencia de uso, preservar la privacidad, garantizar la seguridad, gestionar los riesgos y el fraude, así como asegurar la inclusividad, accesibilidad y usabilidad de los sistemas. Además, deben contemplar procesos de certificación y auditoría.
45. En el ecosistema global existen distintos Organismos normalizadores y Organizaciones que desarrollan especificaciones técnicas, guías o

recomendaciones sobre proyectos de Identidad digital: ISO,¹⁵ NIST (800-63)¹⁶, W3C¹⁷, OECD¹⁸, Banco Mundial ID4D¹⁹, entre otros.

46. Es importante destacar que la consulta pública e involucramiento de todas las partes interesadas en el proceso de creación y actualización de estos marcos de confianza es fundamental para generar confianza gubernamental, empresarial y personal de los usuarios en la adopción y utilización de la herramienta. **La falta de transparencia y consulta pública en este sentido compromete la validez y la legitimidad**

¹⁵ Son varias las normas ISO que están involucradas para establecer reglas de confianza. Como ejemplo, la norma ISO 17065 establece estándares de certificación, validación de conformidad y auditoría. Se puede encontrar la tabla de contenidos de la norma en el siguiente acceso: [ISO/IEC 17065:2012\(es\)](https://www.iso.org/standard/54553.html).

¹⁶ Como precursores en desarrollos de guías en marcos de confianza de identidad digital, en EEUU el National Institute of Standard and Technology U.S. Department of commerce, estableció a partir del año 2006 distintos documentos que sirvieron de apoyo para los desarrollos en Identidad Digital que se fueron dando en ese país y en otras partes del mundo. En el año 2019 la Casa Blanca estableció mediante un memorandum que las normas de identidad, credenciales y acceso del gobierno federal deberán obligatoriamente adoptar la NIST 800-63 <https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf> Se reconocen como: United States NIST 800-63 Digital Identity Guidelines: 2006 800-63, 2011 800-63-1, 2013 800-63-2, 2017 800-63-3, 2023 800-63-4. Se pueden encontrar en el siguiente acceso: [NIST SP 800-63 Digital Identity Guidelines](https://www.nist.gov/publications/nist-sp-800-63-digital-identity-guidelines)

¹⁷ El World Wide Web Consortium (W3C) desarrolla estándares y directrices para ayudar a todos a construir una web basada en los principios de accesibilidad, internacionalización, privacidad y seguridad y bajo esa misión estableció distintas normas: <https://www.w3.org/> Desde el GCABA citaron que el desarrollo en sobre identidad digital que estamos analizando se basó en determinados lineamientos dados por este organismo, en relación puntualmente a la infraestructura descentralizada propuesta, por eso citan en la respuesta que mencionamos en el apartado III. a) esa referencia exclusivamente. No obstante, es observable que la misma norma de W3C en esa materia, deriva sobre ciertas cuestiones mencionadas a normas de otros Organismos normalizadores. por ejemplo, sobre los marcos de nivel de aseguramiento determina que están clasificados y definidos por regulaciones y estándares como eIDAS, NIST 800-63-3 e ISO/IEC 29115:2013, incluidos sus requisitos para el contexto de seguridad y haciendo recomendaciones sobre cómo lograrlos. Es decir, lo importante de los estándares es asegurar que cada desarrollo se respalde en base a ciertos criterios preestablecidos, pero no obstante que cada desarrollo fije sus propias reglas y que queden en claro los procedimientos de manera previa al desarrollo e implementación.

¹⁸ "Recommendation of the Council on the Governance of Digital Identity", Se puede acceder a la guía a través del siguiente enlace: [Recommendation of the Council on Artificial Intelligence](https://www.oecd.org/digital/governance-of-digital-identity/)

¹⁹ Esta Guía fue creada por la "Iniciativa Identificación para el Desarrollo (ID4D) del Banco Mundial". ID4D aporta conocimiento global y experiencia multisectorial para ayudar a los países a aprovechar el potencial transformador de los sistemas de identificación digital (ID). Opera en todo el Grupo del Banco Mundial con prácticas y unidades globales que trabajan en desarrollo digital, protección social, salud, inclusión financiera, gobernanza, género y cuestiones legales. Se puede acceder a la guía a través del siguiente enlace: [ID4D Practitioner's Guide | Identification for Development](https://www.id4d.org/practitioner-guide-identification-for-development/)

de los sistemas de identidad digital implementados por WorldCoin.

47. En efecto, el Banco Mundial en su guía de ID4D recomienda que antes de publicar cualquier tipo de requisitos o lineamientos se debe generar instancias de consulta de multipartes interesadas y Educación²⁰. Asimismo, la OECD recomienda la cooperación entre el sector público y privado para asegurar un ecosistema de identidad digital seguro y eficiente²¹.
48. Además, es relevante señalar que existen referencias de marcos de confianza de identidad digital a nivel mundial, como eIDAS en Europa²², DIATF en Inglaterra²³, PCTF en Canadá²⁴, NIST 800-63 en Estados Unidos²⁵ y TDIF en Australia²⁶, que podrían servir como referencia para establecer un marco adecuado en el caso de WorldCoin.
49. En conclusión, la falta de claridad y transparencia por parte de WorldCoin respecto a las reglas de confianza previas para sus desarrollos de identidad digital representa una preocupación importante en cuanto a la protección de los derechos de los usuarios y la seguridad de los sistemas. La empresa carece de un marco claro y sólido que permita evaluar la debida diligencia, que garantice la confianza y la seguridad de los usuarios en sus sistemas de identificación digital, y permita la participación.
50. Es insuficiente la simple mención a ciertos lineamientos genéricos, tal como lo ha expresado la compañía, pues eso deja a la empresa fuera de todo tipo de evaluación externa en materia de identidad digital, que es uno de los objetivos centrales de su modelo de negocios.

²⁰ Guía ID4D: [ID4D Practitioner's Guide | Identification for Development](#)

²¹ Guía OECD: [Recommendation of the Council on Artificial Intelligence](#)

²² <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281>

²³ <https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-beta-version/uk-digital-identity-and-attributes-trust-framework-beta-version>

²⁴ <https://diacc.ca/trust-framework/>

²⁵ <https://pages.nist.gov/800-63-4/>

²⁶ <https://www.digitalidentity.gov.au/tdif>

V. **LA ACTIVIDAD DE WORLDCOIN. RECOLECCIÓN Y ALMACENAMIENTO DE DATOS ESPECIALMENTE SENSIBLES. PROTECCIÓN NACIONAL:**

51. Según se adelantó, el funcionamiento de WORLDCOIN implica la captura de una imagen de alta resolución del iris de la persona que concurre a los puestos donde se sitúan los orbes que capturan tales fotografías.
52. A cambio de la captura de imagen del iris, la empresa ofrece tokens en criptomonedas al usuario, por un valor que rodea los \$25.000.
53. **ACTUALMENTE SE ESTIMA QUE MÁS DE 200 MIL CHILENOS HAN PARTICIPADO DEL ESCANEO DEL IRIS REALIZADO POR WORLDCOIN.²⁷**
54. Ahora bien, es menester señalar que a través de la captura de imagen del iris, **WORLCOIN tiene acceso a los datos biométricos del usuario que corresponden a datos especialmente sensibles.**
55. La biometría ha sido definida por la autora Lorena Donoso Abarca como:

"El conjunto de técnicas que permiten parametrizar aspectos de la persona que permitan identificarla de manera inequívoca o, al menos, que permitan sostener que existe una alta probabilidad de que se trate de la persona cuya identidad se invoca. En el proceso se captura información de la persona que se tiene a la vista y se compara con aquella que consta en la base de datos en relación a dicha identidad. El sistema arrojará un porcentaje de probabilidad de que trate de la misma persona. En general, el porcentaje de error aceptado dependerá del consenso o las reglas de proceso que se adopten. De esta manera, los sistemas biométricos se evaluarán de acuerdo a su bostez desde el punto

²⁷ <https://www.adnradio.cl/2024/03/13/escaneo-de-iris-de-worldcoin-cuanto-pagan-cuales-son-los-riesgos-y-para-que-usan-la-informacion-que-obtienen-de-mi/>

*de vista técnico, ya sea la cantidad de información que es capaz de capturar y comparar, al porcentaje de coincidencia entre los datos biométricos capturados (menudencia) y los datos que constaban previamente en la base de datos y su posibilidad de realizar validaciones posteriores, entre otros factores”.*²⁸

56. Por su parte, los datos personales se encuentran definidos por el artículo 2 letra f) de la Ley N° 19.628 o “Ley sobre Protección de la Vida Privada (en adelante, “**Ley N° 19.628**”) como aquellos relativos a cualquier información concerniente a personas naturales, identificadas o identificables.

57. Luego, el artículo 2 letra g) de la ley N° 19.628 define los datos sensibles de la siguiente manera:

*“Datos sensibles, aquellos datos personales que se refieren a las **características físicas o morales de las personas** o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual”.*²⁹ (Destacado es nuestro).

58. Al respecto, es menester advertir que **LA CAPTURA DEL IRIS DE UNA PERSONA PERMITE OBTENER DATOS BIOMÉTRICOS QUE SON ESPECIALMENTE SENSIBLES. ELLO, YA QUE EL IRIS ES UNA HUELLA BIOLÓGICA ÚNICA E IRREPETIBLE.**

59. Esta unicidad se debe a la compleja estructura del iris, que se forma a partir de varias capas de tejido. Los patrones de pliegues, hendiduras, y colores son determinados por un proceso aleatorio durante el desarrollo fetal, lo cual resulta en una diversidad casi infinita.

²⁸ Abarca Donoso, Lorena (2022). Comentario al dictamen N°009545n20 de la Contraloría General de la República, en Contreras Vásquez, Pablo et. al., Privacidad y protección de datos personales, jurisprudencia seleccionada y comentada, DER Ediciones. Págs. 173 y 174.

²⁹ Artículo 2 letra (g) de la Ley 19.628.

60. Incluso, en el patrón visual de iris hay más información que identifica unívocamente a una persona que en una huella dactilar.³⁰
61. **En definitiva, WORDLCOIN es una empresa que recolecta y almacena datos especialmente sensibles de las personas que concurren a sus centros. Lo anterior, a cambio de la entrega de criptomonedas.**

VI. REACCIÓN DE OTROS PAÍSES A LA ACTIVIDAD DE WORLDCOIN:

62. Diversos países han manifestado suspicacia ante la legalidad de estas operaciones e iniciado investigaciones que han incluido la orden de detener su funcionamiento y destruir los datos recolectados.
63. Así, la *Commission Nationale de l'Informatique et des Libertés* (Francia) ha señalado que las operaciones de WORLDCOIN parecen cuestionables, y ha iniciado investigaciones en conjunto con la jurisdicción alemana.³¹
64. En el continente africano, una Corte del Estado de Kenia ordenó a WORLDCOIN detener el procesamiento de nuevos datos biométricos en Kenia hasta que se resuelva el caso pendiente contra la empresa por una denuncia presentada por el Comisionado de Protección de Datos de Kenia (DPC). El mismo tribunal ordenó a los demandados la destrucción de todos los datos acumulados bajo la supervisión del DPC.³²

³⁰ RDevincenzi, Finamore, Chichizola y otros. *reconocimiento biométrico de iris en ambientes de alta seguridad*. Facultad de Informática, Universidad Nacional de la Plata (2012).

³¹ Reuters (2023). *France's watchdog questions legality of Worldcoin biometric data collection*: <https://www.reuters.com/technology/frances-privacy-watchdog-says-worldcoin-legality-seems-questionable-2023-07-28/>

³² Jurist (2023). *Kenya High Court halts Worldcoin data processing amid privacy concerns*: <https://www.jurist.org/news/2023/08/kenya-high-court-halts-worldcoin-data-processing-amid-privacy-concerns/>

65. En España, la Agencia de Protección de Datos (AEPD) del país prohibió a Worldcoin seguir escaneando el iris de las personas, interrumpiendo sus operaciones de manera cautelara.³³
66. Finalmente, en Argentina, la Agencia de Acceso a la Información Pública inició una investigación de oficio y conformó un grupo de trabajo sobre la actividad de la empresa a través de la Red Iberoamericana de Protección de Datos.³⁴

VII. DE LA LECTURA DEL IRIS POR PARTE DE NUESTRO REPRESENTADO:

67. El día 13 de marzo de 2023 se encontraba en la ciudad de Viña del Mar, y de manera previa había solicitado una hora a través de la aplicación que tiene WorldCoin con el fin de conocer más del sistema. Meses antes había bajado la aplicación, así que ya la tenía disponible en su teléfono. La dirección que me dieron fue la de "Mall Marina Viña del Mar".
68. Al llegar a este recinto, se percató que la empresa tenía presencia a través de un stand modular muy sencillo en medio de un pasillo del centro comercial, lo que me llamó la atención. Se atendió con uno de los promotores, quien me explicó el funcionamiento de la aplicación, y cómo se obtenía el escaneo del iris a través de un dispositivo que tenían disponible y a la vista del público en ese lugar.
69. Le explicaron que la generación de la identificación digital a través del escaneo del iris se lograba haciendo funcionar al mismo tiempo la aplicación del teléfono junto con el dispositivo de captura biométrico.
70. Abrió la aplicación, y después de aceptar simplemente con una lista de chequeo los términos de uso de la empresa, ya me encontraba en

³³ EFE (2024). La Agencia de Protección de Datos prohíbe a Worldcoin seguir recopilando en España datos del iris. Disponible en: <https://efe.com/economia/2024-03-06/aepd-prohibe-worldcoin-seguir-recopilando-espana-datos-iris/>

³⁴ Gobierno de Argentina (2024). Avanza la investigación de la AAIP sobre WorldCoin y el uso de datos personales. Disponible en: <https://www.argentina.gob.ar/noticias/avanza-la-investigacion-de-la-aaip-sobre-worldcoin-y-el-uso-de-datos-personales>

aquella parte del menu que pedía que me acercara al dispositivo para generar el escaner de su iris.

71. Una vez hecho esto, en la aplicación apareció una bonificación de 10 unidades de criptomonedas de la empresa WorlCoin, equivalente a \$89,999 pesos chilenos. A continuación, le explicaron la forma de convertir esas monedas a pesos y obtener su equivalente en pesos a través de la cuenta RUT del BANCO DEL ESTADO.
72. Como se podrá apreciar en el video que acompañamos en un otrosí, el mecanismo para obtener el consentimiento es muy similar al que se usa para registrarse en cualquier aplicación, y que tiene como opción por defecto el habilitar la posibilidad de transferencia de datos hacia Europa y Estados Unidos. Esto llamó la atención, **pues está fuera de los parámetros de lo que debe ser el consentimiento informado.**
73. Una vez que llega a casa, se puso a revisar más en detalle la información de la compañía, **y se percaó que la información del código de identificación del iris queda registrado en la blockchain, situación de la cual no hay ningún tipo de información visible en la aplicación, lo que vulnera mis derechos.**

VIII. EL ACTO RECURRIDO ES ILEGAL:

74. El acto recurrido, es decir, la recolección por parte de WORLDCOIN de datos biométricos a través de una fotografía del iris ocular a cambio de criptomonedas es ilegal, en atención a los siguientes argumentos:
 - a) **El acto recurrido vulnera el artículo 4 inciso primero y segundo de la Ley N° 19.628:**
75. Según se explicará a continuación, el acto recurrido vulnera el artículo 4 de la Ley N° 19.628, el cual dispone en su inciso primero que: *"el tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello"* (énfasis agregado).

76. Luego, el inciso segundo de dicha norma establece que: “*la persona que autoriza **debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público**” (énfasis agregado).*
77. Es menester señalar al respecto que el consentimiento toma un papel especialmente importante en el tratamiento de datos sensibles, los cuales, por defecto, no pueden ser objeto de tratamiento, pero excepcionalmente pueden serlo, solamente mediante el consentimiento de su titular.
78. En relación a la importancia que le otorga la Ley N° 19.628 al consentimiento debe estarse a los principios generales que la rigen, y al texto propio de su artículo primero, que establece lo siguiente:
- “Toda persona puede efectuar el tratamiento de datos personales, siempre que lo haga de manera concordante con esta ley y para finalidades permitidas por el ordenamiento jurídico. **En todo caso deberá respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que esta ley les reconoce**”.*³⁵ (énfasis agregado).
79. Esta disposición establece que el tratamiento de datos personales -con mayor razón, el de datos sensibles- debe siempre respetar los derechos fundamentales de los titulares de tales datos.
80. La normativa de la Ley 19.628 se remite expresamente, en su artículo primero, inciso segundo, a las reglas y principios relativas a los derechos fundamentales de las personas.
81. **El consentimiento que exige la Ley N° 19.628, entonces, debe ser uno compatible con los derechos constitucionalmente consagrados a todas las personas**, en especial: **(i)** El derecho a la integridad física; **(ii)** El derecho al respeto y protección a la vida privada y la honra; **(iii)** El derecho a la protección de sus datos personales (Artículo 19 N°4 de la CPR); **(iv)** El derecho a la protección

³⁵ Artículo 1, inciso 2° de la Ley 19.628.

de la salud; y, **(v)** El derecho de propiedad sobre toda clase de bienes corporales o incorporales,

82. En materia de protección de datos personales, los/as profesores/as Lorena Donoso Abarca y Carlos Reusser Monsálvez han señalado que el **consentimiento debe ser libre e informado, y que deben tomarse las medidas que permitan que la persona tome conocimiento cabal de los datos que autoriza se traten.**³⁶ En su reciente obra, ambos/as describen el consentimiento en los siguientes términos:

*"La autorización del titular de datos personales como legitimante del tratamiento de datos exige la **adopción de medidas razonables en pos de que el titular de los datos personales tome conocimiento cabal de los datos que autoriza se traten**, cuáles son los mecanismos de recogida, la existencia misma de las operaciones de tratamiento, sus finalidades, responsables, destinatarios de la información, cuánto tiempo se mantendrán en el sistema, y todos aquellos elementos que permitan su correcta identificación y la vigencia de las garantías establecidas en su favor y, por tanto, **se encuentre en condiciones de prestar su consentimiento libre e informado**".*³⁷

83. Respecto al consentimiento debe notarse que existe una gran asimetría entre WORLDCOIN y las personas que acceden a capturar imágenes de su iris por un pago en criptomonedas. Dicho conocimiento **es diametralmente opuesto el grado de conocimientos científicos, legales, y en el poder económico entre las dos partes.**
84. Notando que, en este caso, el de la empresa WORLDCOIN buscando un auténtico consentimiento para lograr un acuerdo: la entrega de datos biométricos en cambio de unas criptomonedas, existe

³⁶ Donoso Abarca, Lorena y Reusser Monsálvez, Carlos (2022). La protección de los datos personales en Chile. Santiago: DER Ediciones. Pág. 85.

³⁷ Donoso Abarca, Lorena y Reusser Monsálvez, Carlos (2022). La protección de los datos personales en Chile. Santiago: DER Ediciones. Pág. 85.

probablemente una mayor asimetría de conocimiento y poder entre la empresa y la persona que concurre a capturar su biometría, este punto se acentúa con mayor énfasis.

85. La importancia de un auténtico consentimiento de las personas que concurren a autorizar el tratamiento de sus datos biométricos no solamente se refleja en los estándares nacionales, sino también en normativa de observancia internacional.

86. Así, las Directrices de la OCDE contienen el llamado principio de limitación de recogida, disponiendo que:

*"Debería haber límites a la recogida de datos personales y cualquiera de esos datos debería ser obtenido por **medios legales y honestos** y, en su caso, **con el conocimiento o consentimiento del sujeto de los datos**".*³⁸ (Destacado es nuestro).

87. Otro principio consagrado en la misma normativa que orienta los estándares internacionales es el de especificación de los fines, mediante su artículo 9:

"Los fines para los que los datos personales se recogen deberían especificarse en el momento en que se recogen, y su uso posterior estaría limitado al cumplimiento de esos fines o de otros que no sean incompatibles con esos fines y se especifiquen cada vez que haya un cambio de fines".

88. Según se adelantó, un aspecto clave del consentimiento es la información. **Solo una persona suficientemente informada es capaz de prestar su consentimiento.** Especialmente ilustrativa es la doctrina sobre el consentimiento informado en la responsabilidad médica, sobre la cual se ha escrito que:

³⁸ Directrices de la OCDE que regulan la protección de la privacidad y el flujo transfronterizo de datos personales, artículo 7°.

*“(...) el respeto a la autodeterminación de los pacientes obliga a los médicos a suministrarles **la información necesaria para que estos puedan decidir si optan por el tratamiento o intervención o no**”.*³⁹

89. Así, la información es una fase previa al consentimiento, y sirve precisamente para arribar a la decisión concreta. Esto se acentúa cuando se ve involucrada la integridad física de una persona o la vida privada y la protección de los datos personales.
90. La información como presupuesto de un auténtico consentimiento va, además, en respeto por la honra de las personas y por su derecho a la propiedad, en este caso, sobre su propia biometría como elemento identitario. Por supuesto, no es posible brindar consentimiento sin comprender aquello en lo cual recae el mismo.
91. Ahora bien, de la lectura de las políticas de privacidad de WORDLCOIN es evidente que los usuarios no se encuentran suficientemente informados respecto del propósito del almacenamiento de sus datos y sus usos.
92. Incluso, según consta en las políticas de privacidad de WORDLCOIN, si estos datos pasan a manos de terceros -que incluso pueden no estar regidos por normas de protección de datos- el usuario no tendrá conocimiento alguno de los usos que se harán respecto a éstos.
93. En definitiva, es evidente que el acto recurrido infringe el artículo 4 de la Ley N° 19.628 ya que el consentimiento que los usuarios prestan para fotografiar su iris no es compatible con los derechos constitucionalmente consagrados.
94. En concreto, dicho consentimiento no es compatible con el derecho a la integridad física, el derecho al respeto y protección a la vida privada y la honra y el derecho a la protección de sus datos personales.

³⁹ Vidal Olivares, Álvaro (2018). Responsabilidad civil médica. Santiago: DER Ediciones. Pág. 45.

b) El acto recurrido vulnera el artículo 11 de la Ley de Protección de datos:

95. El artículo 11 de la Ley de Protección de Datos establece que: *"El responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección **deberá cuidar de ellos con la debida diligencia**, haciéndose responsable de los daños"* (énfasis agregado).

96. Ahora bien, de la mera lectura de las políticas de privacidad de WORLDDCOIN es evidente que la recurrida no cuida con la debida diligencia los datos biométricos obtenidos a través de las fotografías.

97. Al respecto, las políticas de privacidad de la recurrida afirman lo siguiente:

*"Contamos con equipo dedicados a cuidar sus datos y hemos implementado garantías físicas y electrónicas que protegen sus datos tanto en tránsito como en reposo. **Al mismo tiempo, ningún servicio puede ser completamente seguro**".*

98. A mayor abundamiento, WORLDCOIN admite que los datos pueden ser transferidos a lugares donde no se rijan por las mismas leyes de protección de datos. Lo anterior consta en la siguiente imagen:

Cuando usted nos facilita sus datos, estos pueden ser transferidos, almacenados o tratados en un lugar fuera de donde sus datos fueron recopilados originalmente. El país al que se transfieren, almacenan o tratan sus datos puede no tener las mismas leyes de protección de datos que el país en el que usted facilitó inicialmente los datos.

99. Parece especialmente preocupante que la empresa recurrida enumera los posibles riesgos que pueden surgir por la transferencia de dichos datos.

100. Tal como queda acreditado en la siguiente imagen, WORLDCOIN afirma que, en el caso de que los datos sean transferidos a un lugar donde no rijan las políticas de privacidad de datos, **no se podrían hacer valer**

los derechos contra los subcontratistas si éstos trataran ilícitamente sus datos:

- Aunque hacemos lo posible para garantizar que nuestros subcontratistas estén obligados por contrato a proteger adecuadamente sus datos, es posible que estos subcontratistas no estén sujetos a la ley de privacidad de datos de su país. Si los subcontratistas trataran ilícitamente sus datos sin autorización, podría ser difícil hacer valer sus derechos de privacidad contra ese subcontratista. Mitigamos este riesgo al cerrar acuerdos estrictos de tratamiento de datos con nuestros subcontratistas que les obligan a proteger los datos al nivel del RGPD y cumplir con las solicitudes de los interesados.
- Es posible que la ley de privacidad de datos de su país no sea coherente con las leyes de privacidad de datos de los EE. UU. o de la UE. Siempre intentamos cumplir con el más alto estándar de protección de datos al que estamos sujetos. Hasta el momento, consideramos que dicho estándar más alto es el RGPD y tratamos todos los datos como si estuvieran regidos por el RGPD.

101. En atención a las consideraciones anteriormente expuestas, es evidente que WORLDCOIN infringe el artículo 11 de la Ley n° 19.628. Ello, ya que según se acreditó, la empresa recurrida no cuida de los datos biométricos con la debida diligencia.

102. Por el contrario, a través de sus políticas de privacidad, la recurrida permite que terceros -quienes no están regidos por leyes de protección de datos- accedan a estos datos sin limitación alguna.

c) El acto recurrido vulnera el artículo 13 de la Ley N° 19.628:

103. El artículo 13 de la Ley N° 19.628 señala que: "*El derecho de las personas a la información, modificación, **cancelación** o bloqueo de sus datos personales no puede ser limitado por medio de ningún acto o convención*" (énfasis agregado).

104. Ahora bien, según se explicará a continuación, al no asegurar el derecho de nuestro representado a eliminar y cancelar sus datos biométricos de las bases de datos, WORDLCOIN infringe el artículo 13 de la Ley N° 19.628.

105. Para efectos de comprender el contexto de autos S.S. Iltma., se debe considerar que los datos biométricos obtenidos del iris son similares al RUT de cada persona.
106. En efecto, al igual que el RUT, los datos del iris son pasados por un algoritmo el cual los transforma en una secuencia de números conocido como "Hush". Este hush, consistente en una secuencia numérica única, representa entonces al usuario.
107. Luego, los hush ingresan al blockchain, el cual consiste en un libro de contabilidad inmodificable y compartido para registrar transacciones y seguimiento de activos.⁴⁰ En este sentido, todas las transacciones realizadas estarán registradas con el hush del usuario.
108. Tanto el RUT como el hush consisten en una secuencia de números única que pueden ser filtrados e investigados. **En el caso de que dichos números sean seguidos y monitoreados, pueden existir consecuencias graves, ya que podría revelarse la identidad del usuario.**
109. Si bien de acuerdo a las políticas de privacidad de WORLDCOIN, el usuario puede eliminar los datos biométricos obtenidos a través de la lectura del iris, dicha eliminación no impide que estos datos -ahora transformados en hush y presentes en el blockchain- puedan ser monitoreados por terceros.
110. Según se explicó, lo anterior puede producir consecuencias graves y revelar la identidad del usuario.
111. En definitiva, a pesar de que las políticas de privacidad de WORLDCOIN permiten la eliminación de los datos biométricos, la empresa recurrida no elimina dichos datos de la blockchain, del cual -en caso de filtración de datos o monitoreos- se podría obtener la identidad de nuestro representado.

⁴⁰ Información disponible en: <https://www.ibm.com/es-es/topics/blockchain>

IX. EL ACTO RECURRIDO ES ARBITRARIO:

112. Respecto de la exigencia de que el acto recurrido sea arbitrario, asentada jurisprudencia emanada de los Tribunales Superiores de Justicia ha sentenciado que:

*"la arbitrariedad implica **carencia de razonabilidad en el actuar u omitir; falta de proporción** entre los motivos y el fin a alcanzar; ausencia de ajuste entre los medios empleados y el objetivo a obtener, o aun la inexistencia de los hechos que fundamentan un actuar, lo que pugna contra la lógica y la recta razón"* (énfasis agregado).⁴¹

113. Pues bien, es evidente que el acto recurrido sólo obedece al capricho de la empresa recurrida, al comercializar con datos sensibles de las personas que a cambio de una recompensa económica acceden sin ningún conocimiento a escanear su iris.

X. LAS GARANTÍAS FUNDAMENTALES INFRINGIDAS Y VULNERADAS POR LAS ILEGALIDADES Y ARBITRARIEDADES COMETIDAS POR WORLDCOIN:

114. Según se explicará a continuación, el actuar ilegal de WORLDCOIN vulneró el legítimo ejercicio de los siguientes derechos y garantías de nuestro representado, garantizados y amparados en el artículo 20 de la CPR: **(i)** Garantía de que el desarrollo científico y tecnológico estén al servicio de las personas y con respeto a la vida y a la integridad física y psíquica; **(ii)** El derecho a la vida privada, garantizado en el artículo 19 N° 4 de la CPR; y, **(iii)** El derecho a la propiedad, garantizado en el artículo 19 N° 24.

⁴¹ Corte de Apelaciones de Punta Arenas, 22 de septiembre de 1993, Revista Gaceta Jurídica, N° 166, pág. 90; Corte de Apelaciones de Santiago, 05 de marzo de 1992, Revista Gaceta Jurídica, N° 141, pág. 90; Corte de Apelaciones de Santiago 30 de abril de 1.993, Revista Gaceta Jurídica, N° 154, pág. 64; Corte Suprema, 26 de Septiembre de 1.996, Revista Gaceta Jurídica, N° 195, pág. 64

a) **Vulneraciones a la garantía de que el desarrollo científico y tecnológico estén al servicio de las personas y con respecto a la vida y a la integridad física y psíquica:**

115. En virtud de la reforma constitucional de la Ley N° 21.383 se agregó al actual inciso final del artículo 19 N° 1 de la CPR que prescribe: *"El desarrollo científico y tecnológico estará al servicio de las personas y se llevará a cabo con respeto a la vida y a la integridad física y psíquica. La ley regulará los requisitos, condiciones y restricciones para su utilización en las personas, debiendo resguardar especialmente la actividad cerebral, así como la información proveniente de ella"*.
116. Dicha reforma constitucional surgió **a partir de los riesgos que trae aparejado el desarrollo de la inteligencia artificial y que dicen principalmente con el resguardo de la privacidad y la autodeterminación de los individuos, así como reducir los riesgos de discriminación.**⁴²
117. A mayor abundamiento, en la historia de dicha Ley se afirmó que:
- "el desarrollo científico y tecnológico y sus amenazas a la humanidad requiere que el mundo de los derechos humanos enfrente decididamente estos riesgos y desarrolle nuevos derechos humanos acordes a esta nueva realidad"*.⁴³
118. Asimismo, para la dictación de dicha Ley se tuvo en cuenta que hoy en día existe la necesidad de releer derechos como la dignidad humana, la vida privada o la intimidad en atención a las nuevas tecnologías y la ingente capacidad de procesamiento de datos.⁴⁴
119. En definitiva, es evidente que el propósito de la modificación constitucional fue combatir los efectos dañinos que producen las nuevas tecnologías a la privacidad e integridad personal.

⁴² Miralles. Necesidad de proteger constitucionalmente la actividad e información cerebral frente al avance de las neurotecnologías: Análisis crítico de la reforma constitucional introducida por la Ley 21.383 (2021), p. 2.

⁴³ Boletín N° 13.827-19, p. 3.

⁴⁴ Boletín N° 13.827-19, p. 7.

120. Ahora bien, es evidente que, en el presente caso, al ofrecer criptomonedas a cambio de la recolección de datos biométricos de nuestro representado, no proteger adecuadamente dicha información -e incluso retenerla en contra de su voluntad-, la empresa recurrida está vulnerando la garantía establecida en el artículo 19 N° 1 inciso final.

b) Vulneraciones al derecho a la integridad física y psíquica, garantizado en el artículo 19 N° 1 de la CPR:

121. El inciso primero del artículo 19 N° 1 de la CPR señala que, se asegura a todas las personas: "*El derecho a la vida y a la integridad física y psíquica de la persona*".

122. Con respecto a lo anterior, es importante señalar que: "*La integridad psíquica es una dimensión de la persona humana que, junto con la integridad física la integran en plenitud. Ninguna de las dos puede ser descuidada, puesto que ambas componen al individuo en su relación con el entorno social más próximo*"⁴⁵.

123. Según se adelantó, los datos biométricos son datos sensibles los cuales están relacionados con la intimidad de las personas. Su divulgación, por tanto, pone en riesgo al individuo y lo hace susceptible de múltiples afectaciones a sus garantías fundamentales.

124. A mayor abundamiento, **la violación a los datos biométricos de una persona es especialmente grave ya que sus efectos pueden incluso producir una pérdida de identidad.**⁴⁶

125. Tal como quedó acreditado, las políticas de privacidad de de WORDCLOIN son insuficientes para la protección de los datos biométricos de nuestro representado.

126. Por ello, nuestro representado se ve expuesto a los siguientes riesgos:
(i) Reutilización no autorizada de los datos biométricos; **(iv)**

⁴⁵ Vivanco, Ángela. Curso de Derecho Constitucional, Tomo II. 2006, p. 249.

⁴⁶ Quintanilla, Gabriela. Legislación, riesgos y retos de los sistemas biométricos. Revista Chilena de Derechos y Tecnología Vol. 9. Núm 1 (2020).

Mercantilización de los datos biométricos; **(v)** Vigilancia digital; **(vi)** Captación de datos biométricos para fines no consentidos, entre otros.⁴⁷

127. Lo anterior, hace manifiesta la vulneración por parte de la empresa recurrida a la integridad física y psíquica de nuestro representado.

c) Privaciones, perturbaciones y/o amenazas al derecho a la vida privada, garantizado en el artículo 19 N° 4 de la CPR:

128. La captación de información biométrica del iris por parte de la empresa recurrida -la cual no protege adecuadamente dicha información- priva, perturba y/o amenaza el derecho a la vida privada, garantizado en el artículo 19 N° 4 de la CPR.

129. El artículo anteriormente señalado dispone que, se asegura a todas las personas:

"El respeto y protección a la vida privada y a la honra de la persona y su familia, y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley".

130. Es importante destacar que, el Consejo de Derechos Humanos ha reconocido que el derecho a la privacidad es una expresión de la dignidad humana y está vinculado a la protección de la autonomía y a la identidad personal.⁴⁸

131. Asimismo, dicha entidad internacional ha reconocido que las leyes de privacidad de datos constituyen un límite razonable a diversas situaciones negativas como las influencias externas indebidas, la elaboración de perfiles de datos y decisiones automatizadas.⁴⁹

132. Asimismo, en la Resolución A/HRC/55/46 titulada "Mecanismos legales de salvaguarda para la protección de datos personales y la privacidad

⁴⁷ Quintanilla, Gabriela. Legislación, riesgos y retos de los sistemas biométricos. Revista Chilena de Derechos y Tecnología Vol. 9. Núm 1 (2020).

⁴⁸ Consejo de Derechos Humanos. A/HRC/48/31, párr. 7

⁴⁹ Consejo de Derechos Humanos. A/HRC/55/46, párr. 5.

en la era digital” el Consejo de Derechos Humanos afirmó que es especialmente preocupante que en el contexto actual los titulares de datos personales se encuentran en una posición de indefensión por el conocimiento limitado sobre el uso que terceros hacen de dicha información.⁵⁰

133. Ahora bien, debido a que -como se explicó en esta presentación- las políticas de privacidad de WORLDCOIN no protegen adecuadamente la información biométrica de los usuario, es evidente que la recurrida está privando, perturbando y/o amenazando el derecho a la vida privada de nuestro representado.
134. Ello, ya que a pesar de que se trata de información especialmente sensible, luego de la captación de ésta por parte de WORLDCOIN, nuestro representado está expuesto a que sus datos sean vendidos a terceros sin su consentimiento o bien utilizados sin su consentimiento, en contradicción a sus garantías fundamentales.

d) Privaciones, perturbaciones y/o amenazas al derecho a la propiedad, garantizado en el artículo 19 N° 24 de la CPR:

135. El derecho a la propiedad está garantizado en el artículo 19 N° 24 de la CPR, el cual señala que, la CPR asegura a todas las personas: *"el derecho de propiedad en sus diversas especies sobre toda clase de bienes corporales o incorpales"*.
136. Al respecto, es importante destacar nuevamente que, la información biométrica obtenida del iris no constituye cualquier tipo de datos de carácter personal, sino que la información cerebral contiene datos especialmente sensibles de una persona.
137. Según se señaló anteriormente, la información obtenida del iris incluso es más personal y específica que la huella digital.
138. En virtud de lo anterior, aquellas empresas que obtienen datos biométricos -como WORLDCOIN- deben garantizar que la recopilación,

⁵⁰ Consejo de Derechos Humanos. A/HRC/55/46, párr. 10.

el procesamiento y el almacenamiento de dichos datos se realice con especial resguardo.

139. Tal como se señaló anteriormente, las políticas de privacidad de WORLDCOIN son ineficientes y los datos biométricos de los usuarios se encuentran expuestos a grandes riesgos, como el uso no autorizado de dicha información.
140. En atención a lo anterior, es evidente que el derecho a la propiedad de nuestro representado sobre sus datos biométricos está siendo privado, perturbado y/o amenazado por WORLDCOIN.

XI. CONCLUSIÓN:

141. Según quedó acreditado en autos, el acto recurrido, es decir, el escaneo de iris por parte de WORLDCOIN a cambio de criptomonedas es un acto ilegal ya que ingringe: **(i)** El artículo 4 inciso primero y segundo de la Ley N° 19.628; **(ii)** El artículo 11 de la Ley N° 19.628; y, **(iii)** El artículo 13 de la Ley N° 19.628.
142. El acto recurrido, además de ser ilegal, vulnera el legítimo ejercicio de las siguientes garantías fundamentales de las que es titular nuestro representado y que se encuentran amparadas en el artículo 20 de la CPR: **(i)** Garantía de que el desarrollo científico y tecnológico estén al servicio de las personas y con respeto a la vida y a la integridad física y psíquica; **(ii)** El derecho a la vida privada, garantizado en el artículo 19 N° 4 de la CPR; y, **(iii)** El derecho a la propiedad, garantizado en el artículo 19 N° 24.
143. En definitiva, conforme a las normas constitucionales y legales de nuestro ordenamiento jurídico y los argumentos presentados anteriormente, corresponde que S.S. Iltma. acoga la presente acción de protección.

POR TANTO,

SÍRVASE S.S. ILTMA., tener por interpuesta la presente acción de protección en contra de WORDLCOIN, declararla admisible, solicitar informe

al representante legal de la recurrida en Chile a través del correo electrónico fayala@wordlcoin.org dentro del plazo de 5 días y, en definitiva, acogerla en todas sus partes, ordenando lo siguiente: **(i)** Que, la empresa recurrida modifique sus políticas de privacidad en lo concerniente a la protección de los datos biométricos; **(ii)** Que, la empresa recurrida se abstenga de obtener datos biométricos mediante fotografías del iris mientras no modifique sus políticas de privacidad; **(iii)** Que, la empresa recurrida elimine de su base de datos la información biométrica de nuestro representado; **(v)** Que, se adopten todas las demás medidas que se estimen necesarias para restablecer el imperio del derecho; y, **(vi)** Que, se condene expresamente en costas a la empresa recurrida.

PRIMER OTROSÍ: De conformidad a lo dispuesto en el artículo 20 de la CPR, en relación al Numeral 3º inciso final del Auto Acordado, y con el objeto de suspender los efectos del acto recurrido e impedir que éstos se perpetúen en el tiempo, generando un daño irreparable al derecho de privacidad de nuestro representado, venimos en solicitar se decrete orden de no innovar en la presente causa, ordenando que en tanto se tramite la presente acción, WORDLCOIN se abstenga de utilizar -para cualquier fin- sus datos biométricos obtenidos a través de la lectura de su iris.

Lo anterior en virtud de las siguientes consideraciones que a continuación pasamos a exponer:

1. Según se detalló en lo principal de esta presentación, los datos biométricos constituyen datos sensibles los cuales están relacionados con la intimidad de las personas. Su divulgación, por tanto, pone en riesgo al individuo y lo hace susceptible de múltiples afectaciones a sus garantías fundamentales.
2. En este sentido, **la violación a los datos biométricos de una persona es especialmente grave ya que sus efectos pueden incluso producir una pérdida de identidad.**⁵¹

⁵¹ Quintanilla, Gabriela. Legislación, riesgos y retos de los sistemas biométricos. Revista Chilena de Derechos y Tecnología Vol. 9. Núm 1 (2020).

3. Tal como quedó acreditado, **las políticas de privacidad de WORDCLOIN son insuficientes para la protección de los datos biométricos de nuestro representado.**
4. La deficiencia en las políticas de privacidad de la recurrida hace evidente la **urgencia de tomar medidas para que se proteja el derecho a la privacidad de nuestro representado. De lo contrario, éste se ve expuesto a consecuencias dañinas que pueden ser irreversibles para su privacidad.**
5. **La urgencia S.S. Iltma. se refleja en la sensibilidad de los datos que obtiene la empresa, la inexistente información respecto de para que serán utilizados dichos datos obtenidos, y lo señalado respecto de que una vez que dichos datos entren en la blockchain JAMÁS podrán ser eliminados.**
6. Para efectos de lo anterior, solicitamos a esta Iltma. Corte de Apelaciones de Valparaíso que, en virtud de lo expuesto en lo principal de esta presentación, dicte como orden de no innovar lo siguiente: **(i) Que la empresa recurrida se abstenga de obtener datos biométricos mediante fotografías del iris mientras se resuelve el presente recurso;** y/o **(ii) Se dicte cualquier otra medida que S.S. Iltma. estime pertinente para proteger los derechos del recurrente.**

SÍRVASE S.S. ILTMA., acceder a lo solicitado, decretando una orden de no innovar en los términos recién señalados.

SEGUNDO OTROSÍ: Que, por este acto, venimos a acompañar, con citación, copia de los siguientes documentos en que se funda la presente acción de protección:

1. Políticas de privacidad de WORLDCOIN.
2. Programación de cita de nuestro representado con el Orb de WORDLCOIN ubicado en el Mall Marina Viña del Mar agendada con fecha 13 de marzo de 2024.

3. Conjunto de imágenes donde se evidencia la lectura del iris de nuestro representado por parte del Orb de WORDLCOIN.
4. Video de fecha 13 de marzo de 2024 correspondiente a la lectura del iris de nuestro representado por parte del Orb de WORDLCOIN.
5. Print de pantalla de las recompensas económicas obtenidas.
6. Compilado de noticias referidas a las actividades de WORLDCOIN en Chile.

SÍRVASE S.S. ILTMA., tener por acompañados los documentos recién individualizados, con citación.

TERCER OTROSÍ: Sírvase S.S. Iltma. tener presente que en nuestra calidad de abogados habilitados para el ejercicio de la profesión y en virtud de lo dispuesto en el numeral 2º del Auto Acordado sobre Tramitación y Fallo del Recurso de Protección de Garantías Constitucionales de la Excelentísima Corte Suprema, asumimos personalmente el patrocinio y poder en la presente acción de protección, en representación del recurrente, en la que podremos actuar conjunta o separadamente, fijando domicilio en calle Alonso de Córdova 4355, piso 14, Vitacura, quienes firmamos en señal de aceptación.

SÍRVASE S.S. ILTMA., tenerlo presente.

CUARTO OTROSÍ: Sírvase S.S. Iltma. tener presente que para efectos de notificaciones se encuentran habilitadas las siguientes casillas de correos electrónicos: ccolombara@colombara.cl; adiaz@colombara.cl; aalbano@colombara.cl; adelafuente@colombara.cl

SÍRVASE S.S. ILTMA., tenerlo presente.